REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
20-05-2014	Final Report	3-Aug-2012 - 2-Aug-2013

4. TITLE AND SUBTITLE
Data-Dependent Fingerprints for Wireless Device Authentication

5a. CONTRACT NUMBER
W911NF-12-1-0369

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Michael A. Jensen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Brigham Young University
ORCA
A285 ASB
Provo, UT 84602 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
62255-CS-II.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
While authenticating wireless radios based on the unique imperfections in their transmitted waveform has become a topic of some interest, such fingerprinting techniques are vulnerable to an attacker who can listen to a radio's transmission and later mimic the transmission using a sophisticated arbitrary waveform generator. However, this type of vulnerability can be reduced if the authentication is accomplished using a random selection from a long list of possible challenge-response pairs and if the node requesting network access has a fingerprint that changes with each valid response. This work provides a first study of such a concept using a tunable filter used during the

15. SUBJECT TERMS
Authentication, Identity management systems, Access control

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Michael Jensen
UU	UU	UU	UU		19b. TELEPHONE NUMBER 801-422-5736

Report Title

Data-Dependent Fingerprints for Wireless Device Authentication

ABSTRACT

While authenticating wireless radios based on the unique imperfections in their transmitted waveform has become a topic of some interest, such fingerprinting techniques are vulnerable to an attacker who can listen to a radio's transmission and later mimic the transmission using a sophisticated arbitrary waveform generator. However, this type of vulnerability can be reduced if the authentication is accomplished using a random selection from a long list of possible challenge-response pairs and if the node requesting network access has a fingerprint that changes with each valid response. This work provides a first study of such a concept using a tunable filter, used during the authentication exchange, whose tuning voltages are determined from the response data. The work uses simulations and measurements to demonstrate the effectiveness of estimating the distortion function introduced by the tunable filter and using it to identify the device. Results show that the technique can achieve near perfect discrimination between devices and can reject an attacker with very high probability.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper	
05/20/2014	2.00	Attiya Mahmood, Michael A. Jensen. Data-dependent transmitter fingerprints for radio authentication, IEEE Radio and Wireless Symposium. 19-JAN-14, . : ,

TOTAL: **1**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper	
05/20/2014	1.00	Attiya Mahmood, Michael A. Jensen. Design and Statistical Analysis of Data-Dependent Transmitter Fingerprints for Radio Authentication, IEEE Transactions on Wireless Communications (05 2014)

TOTAL: **1**

Number of Manuscripts:

Books

Received Paper

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Attiya Mahmood	1.00	
FTE Equivalent:	**1.00**	
Total Number:	**1**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Michael A. Jensen	0.09	
FTE Equivalent:	**0.09**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

See Attachment

Technology Transfer

Data-Dependent Fingerprints for Wireless Device Authentication

Abstract

While authenticating wireless radios based on the unique imperfections in their transmitted waveform has become a topic of some interest, such fingerprinting techniques are vulnerable to an attacker who can listen to a radio's transmission and later mimic the transmission using a sophisticated arbitrary waveform generator. However, this type of vulnerability can be reduced if the authentication is accomplished using a random selection from a long list of possible challenge-response pairs and if the node requesting network access has a fingerprint that changes with each valid response. This work provides a first study of such a concept using a tunable filter, used during the authentication exchange, whose tuning voltages are determined from the response data. The work uses simulations and measurements to demonstrate the effectiveness of estimating the distortion function introduced by the tunable filter and using it to identify the device. Results show that the technique can achieve near perfect discrimination between devices and can reject an attacker with very high probability.

Index Terms

Authentication, Identity management systems, Access control.

I. Introduction

The management of device identities in a secure network represents a challenging issue, particularly in wireless networks where device identity can be forged by an attacker. While most wireless networks use cryptographic techniques based on secret keys to allow network access only to trusted nodes [1, 2], such key-based authentication either requires tedious and potentially insecure manual entry of public keys in each trusted device or high implementation resource requirements [3–5]. As a result of these limitations, recent work has explored other authentication techniques that can work with and enhance traditional cryptographic authentication methods. Radio frequency (RF) fingerprinting implemented via radiometric device identification [3]-[5] or location-based identification [6]-[8] represent examples of such methods.

Because location-based identification is appropriate only for stationary nodes and static radio propagation environments, most of the recent research has focused on radiometric device identification. This technology relies on the fact that unique imperfections in the components used to construct a transmitter system produce a waveform signature (fingerprint or transceiverprint) that can uniquely identify the device. While the majority of these techniques focus on the waveform achieved during signal transients [4]-[15], more recent work has demonstrated that good identification accuracy is also possible based on the characteristics of the modulated waveform [16, 17]. However, a key vulnerability with this type of authentication is that an attacker can relatively easily capture the waveform characteristics of a radio during its authentication phase and then at a later time masquerade as the legitimate node by using a high-quality arbitrary waveform generator to create an authenticating waveform that mimics that from the legitimate node.

This vulnerability to attack could be reduced if the waveform distortions created by the legitimate node depended on the data being transmitted. In this way, the authentication protocol could involve a large number of possible challenges, each with its own valid response (key). Each legitimate node in the network would then have a unique fingerprint for each challenge-response pair, making it highly unlikely that an attacker could masquerade as a legitimate node based on prior observations. This paper proposes such a technique based on a tunable filter architecture where the tuning voltages can be derived from the response data. A preliminary version of this work was presented in [18], with this current version providing more detailed discussion of the technique along with significantly more data and improved data analysis. The analysis of the experimental data demonstrates that it is possible to have highly accurate identification of the legitimate device with a high probability of rejecting a masquerading device under a variety of assumptions. The results demonstrate that the proposed technique has the potential to significantly enhance the security associated with RF fingerprinting techniques.

II. Fingerprint-Based Authentication

Typically, if a node desires to enter a secure network and participate in the exchange of potentially-sensitive data, it sends a request that is ultimately routed to a decision-making node (DMN), such as an access point in a conventional wireless local area network (WLAN). To verify that the node can be trusted, the DMN transmits a challenge, which is essentially a request for information that only trusted nodes possess. The requesting node (RN) seeking network access must then supply the proper response to the challenge, a response that may be a pre-shared security key, a known MAC address, or some other secret information. Upon receipt of the correct information, the RN is considered authentic and is allowed to use the network resources.

While this conventional authentication is simple, it is relatively easy for an attacker to either gain the secret information or to supply the credentials of another radio to gain network access. Because of this vulnerability, some researchers have proposed

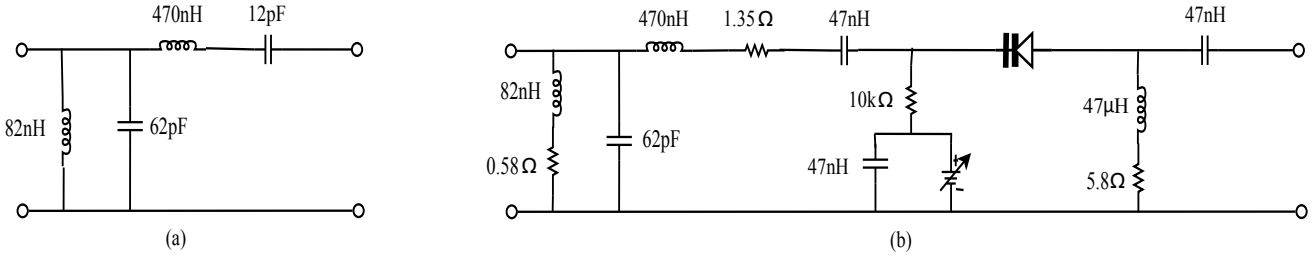

Fig. 1. (a) Design of a second-order bandpass filter used as a fundamental building block in this work. (b) Implementation of the second-order bandpass filter including inductor losses, the series capacitance replaced with a varactor diode, and the required bias circuitry to varactor diode tuning.

combining this type of typical authentication with techniques at the physical layer that may be harder to imitate. For example, fingerprint-enhanced authentication exploits the fact that analog circuitry in a transceiver is characterized by imperfections that create unique properties of the transmitted waveform. Key aspects of the waveform are therefore experimentally characterized for each radio, and these properties are stored in a database available to the DMN. When the RN provides a response to the challenge, the DMN ensures that 1) the response is correct and 2) the properties of the waveform conveying the response match the properties stored in the database for the specific radio, with network access granted only when both of these criteria are satisfactorily met. Prior work on this topic demonstrates that this type of radio fingerprinting can lead to very reliable authentication [16], with the performance improving when the RN has multiple independent transmit circuits [17].

While such fingerprint-enhanced authentication improves security, if an attacker listens to the authentication exchange for a specific radio, it can use sophisticated equipment to carefully measure the waveform. Later, this attacker can use an arbitrary waveform generator to imitate the observed waveform and successfully masquerade as the legitimate node. This observation motivates the concept of data-dependent fingerprints for overcoming this vulnerability. Specifically, suppose that the DMN has a large number of challenge-response pairs that it can use to authenticate a RN seeking network access and further suppose that for each response, the physical properties of the RN transmitter circuit and therefore the transmitted waveform change. Then even if an attacker can 1) know the proper response to a challenge and 2) mimic the waveform observed from observations of prior responses, it does not know the waveform to apply for the current response. We note that if there are enough challenge-response pairs and if authentication is done somewhat infrequently, this concept of data-dependent fingerprints has similarities to the concept of a one-time pad used in data cryptography [1], as the waveform achieved is different for each authentication exchange.

Making the transmitted waveform distortion depend on the transmitted data means that the transmitter is either nonlinear or time-variant (or both). For example, the nonlinear power amplifier in a transmitter will create distortions that depend on the transmit waveform, with the sensitivity to the waveform enhanced when using a modulation based on orthogonal frequency division multiplexing (OFDM) that has a large range of signal levels. However, in implementing authentication based on data-dependent fingerprints, it is essential that 1) the waveforms for different responses be sufficiently distinct to allow differentiation by the DMN and 2) the waveforms achieved by different radios for the same response data be sufficiently distinct to minimize the risk that an imposter can gain network access. As we have explored the use of amplifier nonlinearity to create data-dependent fingerprints, we have found that the nonlinear behavior of different amplifiers (all of the same model) driven into saturation is similar, making discrimination of different devices (objective # 2) difficult.

III. Time-Variant Filter Design

Motivated by the difficulties associated with using nonlinearity to create a data-dependent fingerprint, in this paper we focus on using a time-variant system to create the data-dependent fingerprint, with the time-variation controlled by the data itself. Specifically, we design a filter with selected capacitors replaced by varactor diodes. Our work focuses on a radio frequency (RF) of 2.4 GHz, and therefore we have explored designing a filter at this RF. However, for a usable bandwidth of 20 MHz, the fractional bandwidth achieved at the center frequency of 2.4 GHz is so narrow that it is difficult for the filter to generate appreciable variation of the filter distortion function as a function of frequency. As a result, we instead report on a filter designed at an intermediate frequency (IF) of 70 MHz. The following sections discuss the design, simulation, and experimental implementation of the filter used.

A. Filter Design and Simulation

Naturally, a filter of arbitrary order can easily be designed using conventional filter synthesis techniques and then selected components can be replaced with tunable capacitances. For simplicity in this study, we have chosen to design a simple second-order bandpass filter as a building block for the study. Figure 1(a) shows the schematic of this second-order filter designed for a center frequency of 70 MHz. The ohmic loss components are included to model the equivalent series resistance present in the actual inductors used in filter fabrication.

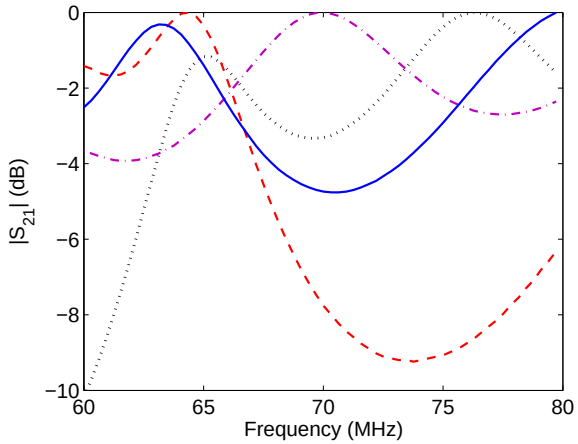

Fig. 2. Simulated $|S_{21}|$ as a function of frequency of an eighth-order filter at four different bias voltage combinations.

To make the distortion function of this circuit tunable, the series capacitor is replaced with a varactor diode with a bias circuit such that the achieved capacitance can be specified by the bias voltage. Figure 1(b) shows this implementation, including the components used for the biasing circuit. Because the series inductor/capacitor combination operates near resonance, small changes in the varactor capacitance can dramatically impact the achieved filter distortion function. The varactor diode chosen for the application is the Skyworks SMV1236, which is a silicon hyperabrupt junction device with a high quality factor. The device's capacitance range is approximately 27-6 pF for a bias voltage range of 0-5 V [19].

To increase the sensitivity of the achieved filter distortion function versus bias voltage, we have cascaded four copies of the second-order filter block. The resulting eighth-order circuit has been simulated using Agilent Advanced Design System (ADS), with the varactor modeled based on the manufacturer equivalent circuit [19]. Figure 2 shows the magnitude of the transmission S-parameter S_{21} obtained from this eighth-order circuit for four different arbitrarily-chosen bias voltage combinations (all chosen in the range 0-5 V) applied to the tunable capacitances. The results clearly demonstrate wide variation in the achieved filter distortion function for different bias voltages, suggesting that this type of circuit is a reasonable candidate for achieving a data-dependent distortion function.

B. Hardware Implementation

The eighth-order circuit (resulting from cascading four second-order filters) has been fabricated using a coplanar waveguide design on Rogers R4003C substrate. To allow assessment of the unique variations created by different circuits, two different copies of the circuit were created. Figure 3 shows a photograph of one eighth-order module where each second-order circuit is bounded with dashed lines. Key components for one of the second-order circuits are also identified in the photograph. Figure 4 plots $|S_{21}|$ as a function of frequency for this eighth-order design measured using a vector network analyzer for four different bias voltage combinations. The curves have been normalized to a maximum value of unity, as the relative variation with frequency for different vias voltages is the key behavior that enables data-dependent fingerprinting and differences in absolute levels will ultimately be combined with propagation path loss and in some cases will be mitigated using transmit power control. Due to the inherent imperfections in the diode behavior with bias voltage and the parasitics introduced during fabrication, the measured filter distortion functions differ from those predicted by the simulations (compare to Fig. 2). However, the basic nature of the filter transfer function variation (rate of change with frequency and relative increase in insertion loss) observed for the measured circuit is similar to that observed in the simulations. The simulated and measured results clearly demonstrate that the tunable circuit is able to introduce significant variations in the distortion function with frequency, further suggesting that this type of circuit may be effective in providing a data-dependent fingerprint.

As previously mentioned, for data-dependent fingerprinting, the distortion function of two different circuits must differ even when both use the same bias voltage combinations. Figure 5 plots $|S_{21}|$ versus frequency when the two fabricated circuits use the same bias voltages, where each subplot represents a unique bias voltage combination. Clearly, these functions for the two circuits differ significantly as a result of the uniqueness of the varactor diode behavior, further reinforcing the suitability of this type of structure for data-dependent fingerprinting.

IV. Authentication Protocol Implementation

The prior section demonstrates that the tunable filter proposed can produce unique distortion functions for different bias voltage combinations and that different circuits fabricated with the same components provide unique distortion functions for the same bias voltage combinations. We are now prepared to discuss how to use this basic architecture to assist in authentication

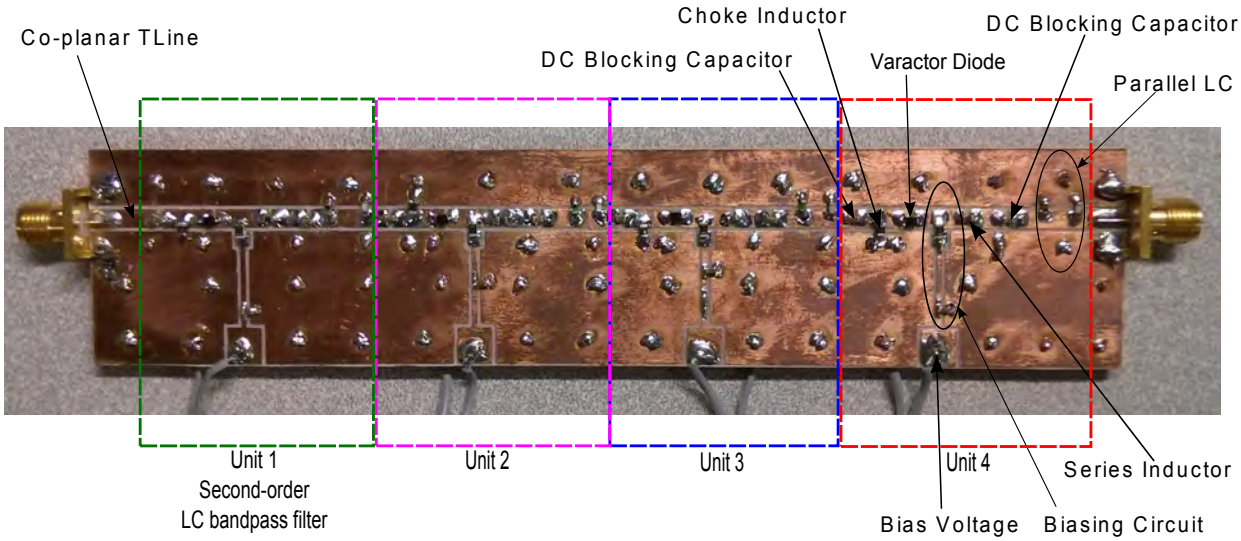

Fig. 3. Photograph of the fabricated eighth-order LC bandpass filter identifying the key components used in the design.

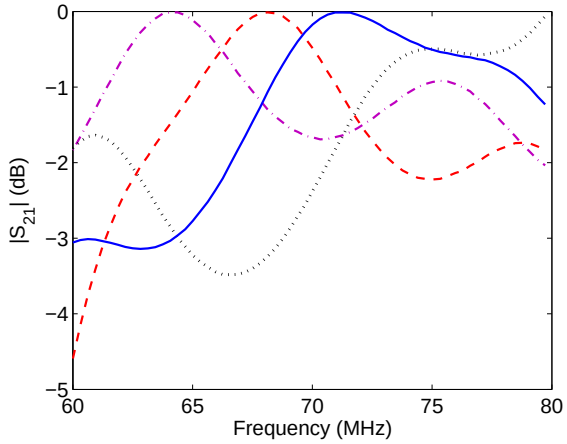

Fig. 4. Measured $|S_{21}|$ as a function of frequency of an eighth-order filter at four different bias voltage combinations.

using data-dependent fingerprints. In the authentication protocol, we assume that the RN transmitter creates an IF waveform with a bandwidth of 20 MHz centered at 70 MHz. The radios use OFDM with 64-point FFT block sizes for transmission so that the bandwidth is divided into $N_{\rm d} = 64$ data and $N_{\rm c} = 5$ cyclic prefix samples. Each tone is modulated using quadrature phase shift keying (QPSK) with a symbol period of $T_{\rm s} = 3.45\mu$s that includes the cyclic prefix of duration $T_{\rm c} = 0.25\mu$s.

Figure 6 diagrams the key elements of the authentication protocol proposed. As previously mentioned, the protocol includes a standard challenge-response exchange, but where the transmitter filter distortion function depends on response data. To enhance the security of the approach, there should be a large number of challenges with a corresponding set of unique responses so that an attacker is unlikely to observe the same response (and corresponding filter distortion function) multiple times. In our analysis, the same challenge-response pair is never repeated. The following sections detail the steps used to achieve authentication based on the data-dependent filter distortion based on the exchanges shown in Figure 6.

A. Propagation Channel Estimation

When the RN requests network access, the DMN requests that the RN transmit training data. Because the objective of this training data transmission is to allow the DMN to estimate the current propagation conditions between the radio, the RN transmission is accomplished *without the tunable filter in the signal path*. We model the channel by a complex impulse response in the delay variable τ given by

$$c_{\rm p}(\tau) = \sum_{\ell=1}^{L} \alpha_\ell \delta(\tau - \tau_\ell T_{\rm s}) \tag{1}$$

where $T_{\rm s}$ is the OFDM symbol period (and therefore discrete-time sampling period) and L is the number of multipaths in the channel with the ℓth multipath modeled as having a complex gain α_ℓ and delay $\tau_\ell T_{\rm s}$. This continuous-time impulse response

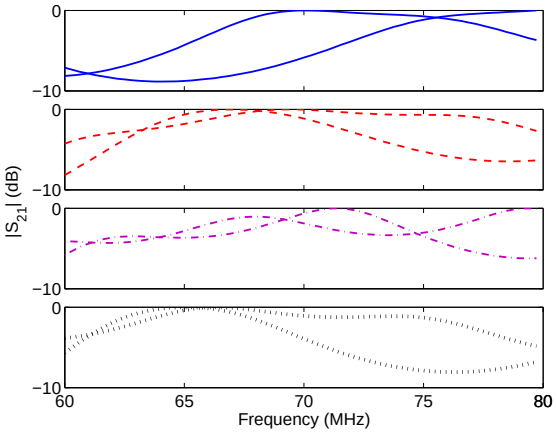

Fig. 5. Measured $|S_{21}|$ as a function of frequency of two eighth-order circuits at four different bias voltage combinations.

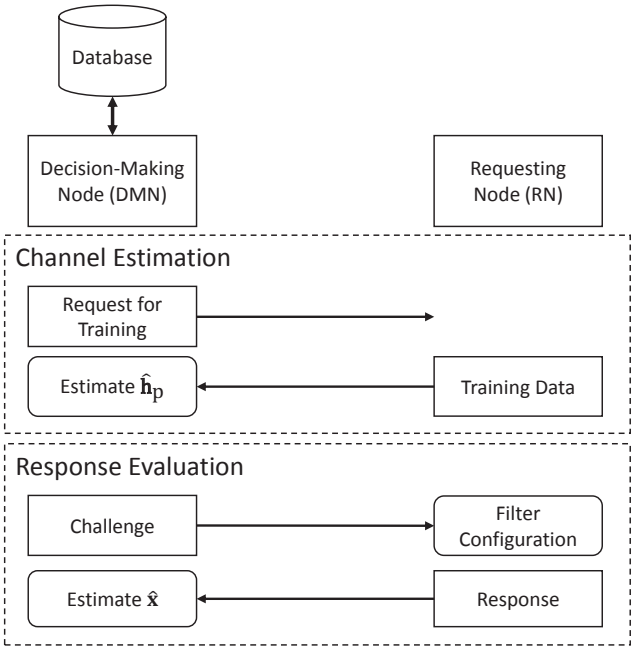

Fig. 6. Block diagram of the exchanges required for authentication based on a data-dependent filter distortion function.

can be converted to a discrete-time form suitable for use with our OFDM implementation by sampling the Fourier transform of $c_\mathrm{p}(\tau)$ and applying an N_d-point inverse Discrete Fourier Transform (DFT) to obtain the discrete-time impulse response vector $\mathbf{g}_\mathrm{p}$, as detailed in [20]. The vector of complex channel gains at the OFDM frequencies is then given by $\mathbf{h}_\mathrm{p} = \mathrm{DFT}_{N_\mathrm{d}}(\mathbf{g}_\mathrm{p})$.

Given this channel description, the data transmitted during a symbol time can be represented by a N_d-length vector. To enable formulation in matrix notation, we form the $N_\mathrm{d} \times N_\mathrm{d}$ matrix $\mathbf{X}_\mathrm{t}$ whose diagonal elements represent the training data symbols. The vector $\mathbf{y}_\mathrm{t}$ of received signals can then be expressed as

$$\mathbf{y}_\mathrm{t} = \mathbf{X}_\mathrm{t}\mathbf{h}_\mathrm{p} + \mathbf{n}_\mathrm{t}, \tag{2}$$

where $\mathbf{n}_\mathrm{t}$ is a vector of independent identically distributed Gaussian noise.

From the received signal vector, the DMN must estimate the propagation channel response $\mathbf{h}_\mathrm{p}$. For line-of-sight (LOS) channels ($L = 1$), least squares (LS) provides an effective estimation approach. This estimate can be formulated using [20]

$$\hat{\mathbf{h}}_\mathrm{p} = \mathbf{X}_\mathrm{t}^{-1}\mathbf{y}_\mathrm{t} \tag{3}$$

where $\hat{\mathbf{h}}_\mathrm{p}$ is the estimate of the propagation channel transfer function. For non-line-of-sight (NLOS) channels ($L > 1$), a minimum-mean-squared-error (MMSE) approach provides a more accurate estimate of $\hat{\mathbf{h}}_\mathrm{p}$ [20]. This estimate relies upon knowledge of the autocovariance of $\mathbf{g}_\mathrm{p}$, as detailed in [20], and therefore it is assumed that the system can use adequate training to achieve this autocovariance estimate.

B. Response Evaluation

Once the propagation channel estimate has been obtained, the DMN sends a challenge to the RN. The RN looks up the correct response to the challenge and inputs the response data to a mapping function that creates a unique bias voltage combination for the varactor diodes in the tunable filter. The RN then switches the biased filter into the transmission signal path and transmits the response data to the DMN, where we assume that the response requires $N_{\rm r}$ OFDM transmissions each of which conveys $N_{\rm d}$ information symbols. With the tunable filter included, the ith received OFDM signal vector at the DMN can be expressed as

$$\mathbf{y}_i = \mathbf{X}_i \left(\mathbf{h}_{\rm f} \odot \mathbf{h}_{\rm p}\right) + \mathbf{n}_i \tag{4}$$

where $\odot$ indicates a Hadamard (element wise) product, $\mathbf{X}_i$ is a diagonal matrix containing the response data elements, and $\mathbf{h}_{\rm f}$ is the distortion function of the eighth-order bandpass filter.

At this stage, the DMN must extract the information necessary to determine whether or not it believes the RN is authentic. Conceptually, this means both estimating the filter distortion function $\mathbf{h}_{\rm f}$ and ensuring that the transmitted data is the correct response for the challenge. From a practical standpoint, however, without additional data transmitted from the RN to the DMN, there is no way to correctly establish one of these two quantities unless the other is correct. Therefore, a simple way to detect whether or not the RN is authentic is to assume that the filter distortion function $\mathbf{h}_{\rm f}$ contained in the database accessible by the DMN is correct and using it to estimate the transmitted data. Let $\mathbf{x}_i$ represent the response data vector (diagonal elements of $\mathbf{X}_i$) and $\hat{\mathbf{x}}_i$ indicate the estimate of this vector created by the DMN for an assumed value of $\mathbf{h}_{\rm f}$ retrieved from the database. Given that the DMN has already estimated the propagation channel $\hat{\mathbf{h}}_{\rm p}$, this data estimate can be computed using

$$\hat{\mathbf{x}}_i = \mathbf{y}_i \oslash \left(\mathbf{h}_{\rm f} \odot \hat{\mathbf{h}}_{\rm p}\right) \tag{5}$$

where $\oslash$ is an element wise division operator. We will use $\mathbf{x}$ to indicate the $N_{\rm r}N_{\rm d} \times 1$ composite vector containing the response symbols with $\hat{\mathbf{x}}$ indicating its estimate.

While all authentication decisions are made based on the estimate $\hat{\mathbf{x}}$ of the response vector, for some of the analysis we wish to understand properties of the estimates of the filter distortion function assuming that the correct response data has been transmitted. Then the DMN can estimate the filter distortion function from this data using

$$\hat{\mathbf{h}}_{{\rm f},i} = \left[\mathbf{X}_i^{-1}\mathbf{y}_i\right] \oslash \hat{\mathbf{h}}_{\rm p} \tag{6}$$

for $1 \le i \le N_{\rm r}$. The estimates $\hat{\mathbf{h}}_{{\rm f},i}$ are then averaged to obtain the filter distortion function estimate $\hat{\mathbf{h}}_{\rm f}$.

C. Authentication Decision

To determine device authenticity, we compare the estimate $\hat{\mathbf{x}}$ to the correct response symbols $\mathbf{x}$ using a mean-squared difference (MSD) metric computed as

$$\text{MSD}_{\mathbf{x}} = \frac{1}{N_{\rm d}N_{\rm r}} \|\mathbf{x} - \hat{\mathbf{x}}\|_{\rm F}^2 \tag{7}$$

where $\|\cdot\|_{\rm F}$ is the Frobenius vector norm. One simple approach for authentication is to simply require that $\text{MSD}_{\mathbf{x}}$ be less than a threshold $\text{MSD}_{\rm th}$. However, more robust rejection of imposter devices can be accomplished if we compute $\hat{\mathbf{x}}$ for *each* of the possible values of $\mathbf{h}_{\rm f}$ in the database for the device. Then, the device is considered authentic only if the MSD achieved with the correct filter distortion function is below the threshold **and** is smaller than the MSD obtained with any other distortion function. Such an approach will be considered in the analysis in Section V.

V. Results

We are now prepared to explore the effectiveness of the authentication protocol when applied to the OFDM-based communication system using measured distortion functions from the two fabricated eighth-order tunable filters. For each fabricated filter, we collected filter distortion functions (four of which appear in Figure 4) for 100 different bias voltage combinations. It is assumed that the mapping function that matches the correct response data to the bias voltage combination is programmed to achieve the bias voltages corresponding to these distortion functions, meaning that our system has 100 different challenge-response pairs.

For the simulations, the NLOS channel is modeled using (1) with $L = 5$ multipath components where $\tau_1 = 0$ and τ_ℓ for $2 \le \ell \le L$ are independent random variables drawn from a uniform distribution on $(0, \xi]$ with $\xi = T_{\rm c}/T_{\rm s} = 0.0725$ so that the delay spread of the multipath components is less than the duration $T_{\rm c}$ of the cyclic prefix. The multipath gains are generated using $\alpha_\ell = \exp(-4\tau_\ell/T_{\rm c})$. A total of $50,000$ realizations of the channel are generated from which the autocovariance of $\mathbf{g}_{\rm p}$ is computed using the procedure detailed in [20]. The LOS channel is modeled simply by taking the first component from the multipath channel ($\tau_1 = 0$ and $\alpha_1 = 1$).

We assume that the average power of the signals transmitted by the RN is normalized to unity, and we define the average signal-to-noise ratio (SNR) per symbol as

$$\text{SNR} = \frac{1}{N_{\rm d}\sigma_n^2} \|\mathbf{h}_{\rm p} \odot \mathbf{h}_{\rm f}\|_{\rm F}^2 \tag{8}$$

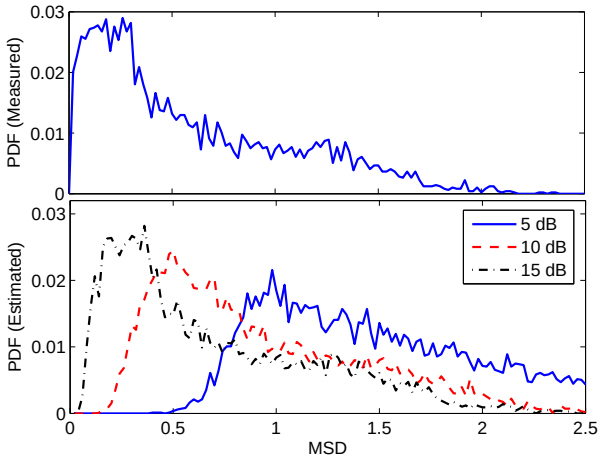

Fig. 7. PDF (approximated using a normalized histogram) of the MSD between all pairs of measured (top) or estimated (bottom) channel distortion functions, where three different SNR values are used when propagation channel estimation is considered.

where σ_n^2 is the variance of each element of the noise vector. For the simulations, we realize $10,000$ different noise vectors from a complex Gaussian distribution for each SNR value and for each noise realization we transmit all 100 responses, each using its corresponding filter distortion function. For each transmission, the DMN estimates $\hat{\mathbf{x}}$ for each of the 100 possible distortion functions in its database and computes the MSD between each estimate and the correct response vector $\mathbf{x}$ using (7), with the result allowing application of the authentication protocol discussed in Section IV-C. The resulting $10,000$ realizations allow a statistical analysis of the probability of correct authentication as well as of denying authentication to an imposter, as detailed in the following subsections.

A. Filter Distortion Functions

It is first interesting to explore the difference between the 100 filter distortion functions measured from one of the fabricated filters. We quantify the difference between a pair of functions using the MSD computed as

$$\mathrm{MSD}_{\mathbf{h},mn} = \frac{1}{N_\mathrm{d}} \|\mathbf{h}_{\mathrm{f},m} - \mathbf{h}_{\mathrm{f},n}\|_\mathrm{F}^2 \tag{9}$$

where the subscripts $\{m, n\}$ indicate the index of the measured distortion function (out of 100). The top plot in Figure 7 shows the probability density function (pdf) approximated as a normalized histogram for all pairwise combinations of the measured distortion functions (except $m = n$). The bottom plot shows similar histograms obtained for estimates of the channel distortion function obtained when the protocol of Figure 6 is used (based on the originally-measured transfer functions) in NLOS conditions for three different SNR values. As can be seen, most of the distortion functions have an MSD larger than 0.5, although the fraction of pairs with such a difference decreases as the SNR increases. These results suggest that the filter distortion functions are generally adequately different to offer the potential of robust data-dependent device identification.

B. Authentication Performance

A device is considered authentic only if $\mathrm{MSD}_\mathbf{x}$ computed using the correct filter distortion function is below the threshold MSD_th *and* lower than $\mathrm{MSD}_\mathbf{x}$ computed using the other distortion functions available in the database for that device. With more available challenge-response pairs, there is an increased probability that an incorrect filter distortion function leads to the lowest value of $\mathrm{MSD}_\mathbf{x}$, and we therefore consider authentication using subsets of 50 and 75 of the distortion functions as well as using all 100 functions. Figure 8 plots the probability of correct authentication as a function of the threshold MSD_th using SNR values of 5, 10, and 15 dB for both LOS and NLOS propagation channels. The results show that for high SNR and an adequately-large threshold, the probability of correct authentication is reasonably high for LOS channels. However, for NLOS channels, errors in the propagation channel estimate reduce the probability of correct authentication relative to the performance observed for LOS conditions. The results also demonstrate that, at least for the number of responses used here, having more filter distortion functions available does not significantly impact the results.

For all cases in Figure 8, it is seen that the performance dependence on the threshold is small once the threshold reaches a certain value. For threshold values beyond this point, if a legitimate device is not authenticated, it is because the MSD for an incorrect filter distortion function is smaller than that achieved with the correct distortion function. This means that very high probability of correct authentication could be achieved if the authentication protocol only requires the MSD to be below a certain threshold. However, simplifying the protocol in this manner also produces a much higher probability of rejecting an imposter. More detail on this observation will be provided in the following section.

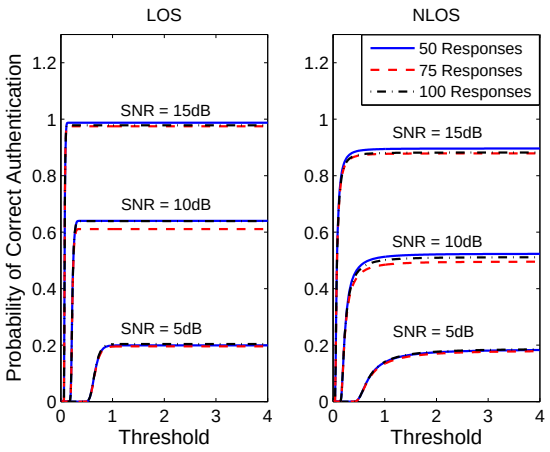

Fig. 8. Probability of correct authentication versus decision threshold in LOS and NLOS channels for three different SNR values and three different numbers of available challenge-response pairs.

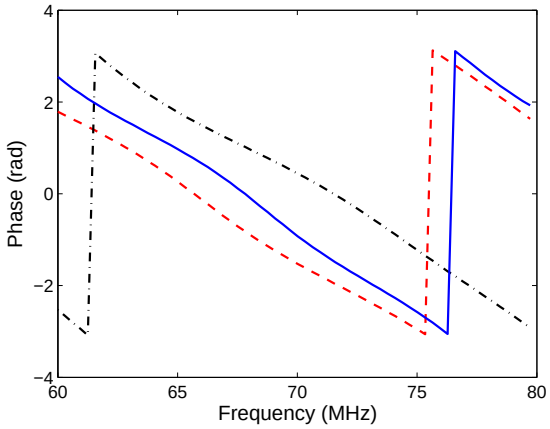

Fig. 9. Measured phase as a function of frequency of the eighth-order filter distortion function for three different bias voltage combinations.

C. Imposter Rejection

In analyzing the ability to reject an imposter attempting to masquerade as a legitimate device, it is important to consider the amount of information known by the imposter. In all cases, we assume that the imposter knows the correct response to the challenge issued by the DMN. The following sections study the ability to reject this imposter under scenarios where the imposter may also know additional information regarding the legitimate RN.

1) CASE I: Attacker Knows Filter Delay: While plots of filter distortion functions used in this paper focus on the magnitude of the filter transfer function, clearly the phase of the transfer function also plays a role in determining the MSD of the estimated response data vector. However, over the frequency band of interest, the phase variation is relatively simple. For example, the curves in Figure 9 show the phase of $\mathbf{h}_{\mathrm{f}}$ versus frequency for three different bias voltage combinations. The results not only show that the phase is relatively linear with frequency, but that the slope of this line is similar for all networks. Therefore, if the attacker listens to several authentication responses, it may be able to infer this slope and better imitate the phase variation of the actual filter.

To investigate the potential impact of this awareness, we determine the average slope of the phase with frequency for all 100 filter distortion functions and compute the average slope. We then assume that the attacker creates a filter distortion function whose phase with frequency is linear with this average slope. We assume that the attacker knows only the slope and therefore applies a uniformly distributed random phase offset to form the imitating distortion function. The magnitude of the imitating function is formed by randomly selecting the magnitude from one of the 100 measured distortion functions.

Figure 10 plots the probability of rejecting an imposter device as a function of the threshold value $\mathrm{MSD}_{\mathrm{th}}$ assuming 50, 75, and all 100 filter distortion functions are available and for three different values of the SNR. The results show that, provided the threshold is chosen to be adequately small, the probability of imposter rejection remains very high for all simulation scenarios. Therefore, attacker awareness of the average slope of the phase versus frequency for the distorting filter provides little if any additional vulnerability.

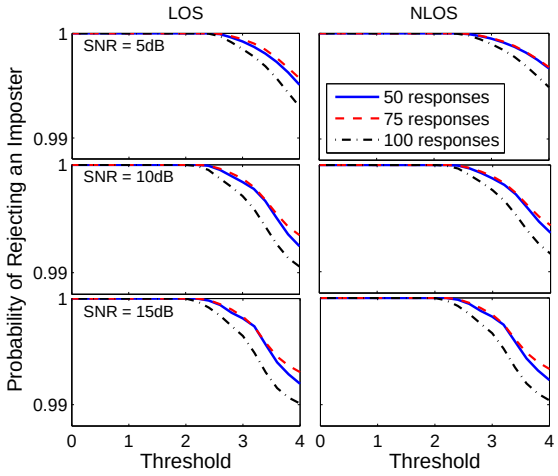

Fig. 10. Probability of rejecting an imposter device as a function of the decision threshold for LOS and NLOS channels when the imposter knows the average slope of the phase versus frequency of the filter distortion function.

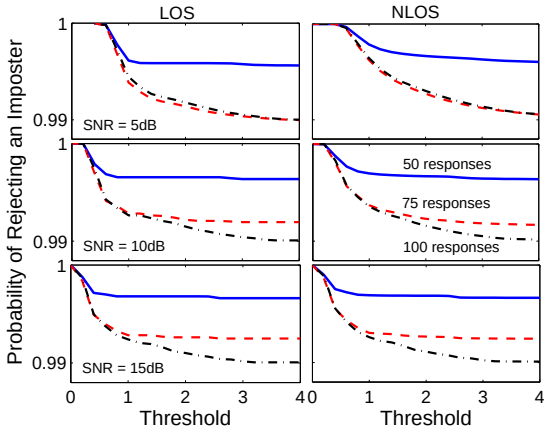

Fig. 11. Probability of rejecting an imposter device as a function of the decision threshold for LOS and NLOS channels when the attacker knows the circuit design but not the bias voltage combinations associated with each challenge-response pair.

2) CASE II: Attacker Knows the Circuit Design: Next, we assume that the attacker is able to reproduce the circuit used by the legitimate device to change the filter distortion function but does not know the mapping function between each valid response and the bias voltages applied to the varactor diodes. To investigate this case, the 100 filter distortion functions measured from the second fabricated eighth-order filter are assumed to be those that can be used by the attacker. These distortion functions are measured for the same bias voltage configurations as those used for the measurements of the filter used by the legitimate node. Because the imposter does not know the mapping function between the response and the bias voltages, we assume that the attacker randomly selects a distortion function when responding to each challenge.

Figure 11 plots the probability of rejecting the imposter device as a function of the decision threshold for the same parameters as used previously. While the results show that the probability of rejection remains quite high (above 99% for most scenarios), the decrease in performance occurs at a much lower threshold than that observed in Figure 10, simply because the imposter sometimes will use a filter distortion function that is close enough to successfully be authenticated. For the same reason, using 75 or 100 responses decreases the probability of imposter rejection, as in these cases the imposter has more filter distortion functions from which to choose.

3) CASE III: Attacker Knows the Circuit Design and Bias Voltages: In the final scenario considered, the attacker has fabricated a filter whose design is identical to that used for the legitimate node and knows the bias voltages used for each challenge-response pair. In this case, only unique differences in the designs lead to different filter distortion functions observed for the legitimate and the imposter radios. Transmissions from the imposter node are again represented using the 100 distortion functions measured from the second filter for the same bias voltages used for the filter on the legitimate node. Figure 12 plots the probability of rejecting the imposter device as a function of the decision threshold. It may appear surprising that the performance in this case is superior to that achieved when the imposter does not know the bias voltages. This indicates that

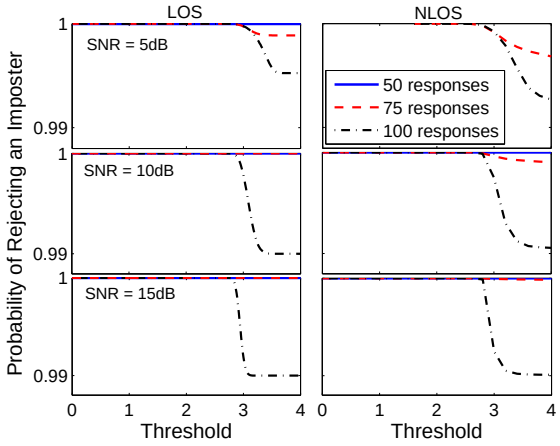

Fig. 12. Probability of rejecting an imposter device as a function of the decision threshold for LOS and NLOS channels when the attacker knows the circuit design and the bias voltage combinations associated with each challenge-response pair.

when the imposter carefully attempts to reproduce the filter distortion function by matching the bias voltage configurations, the unique diode characteristics make it highly likely that a significant mismatch in achieved distortion functions will occur. However, when the attacker randomly chooses a filter distortion function, there is a higher likelihood that the attacker will be fortunate enough to select a function that is adequately close to the distortion function used by the legitimate node.

REFERENCES

[1] W. Stallings, *Cryptography and network security: principles and practice*, 3rd ed. Prentice Hall, 2003.

[2] C. Chen, "Secret key establishment using wireless channels as common randomness in time-variant MIMO systems," Ph.D. dissertation, Brigham Young University, 2010. [Online]. Available: http://contentdm.lib.byu.edu/u?/ETD,2083

[3] M. Barbeau and J.-M. Robert, "Perfect identity concealment in UMTS over radio access links," in *Proc. IEEE Intl. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob)*, vol. 2, Montreal, Canada, Aug. 22-24 2005, pp. 72–74.

[4] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in *Proc. Mobile Ad-hoc Networks and Sensors (MADNES) - Workshop on Secure Mobile Ad-hoc Networks and Sensors (Singapore, Sep. 20-22, 2005)*, vol. 4074. Springer Lecture Notes on Computer Science, 2006, pp. 80–95.

[5] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. of the IEEE Transactions on Information Forensics and Security (ICC)*, Jun. 2007, pp. 4646–4651.

[6] N. Patwari and S. K. Kasera, "Temporal link signature measurements for location distinction," *IEEE Trans. Mobile Computing*, vol. 10, pp. 449–462, Mar. 2011.

[7] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proc. of the 13th annual ACM international conference on Mobile computing and networking (ACM MOBICOM)*, Spetember 2007, pp. 111–122.

[8] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *ACM Workshop on Wireless Security (WiSe)*, Los Angeles, CA, Sep. 29 2006, pp. 43–52.

[9] H. C. Choe, C. E. Poole, A. M. Yu, and H. H. Szu, "Novel identification of intercepted signals from unknown radio transmitters," in *SPIE: Wavelet Applications II*, H. H. Szu, Ed. SPIE, 1995, vol. 2491, pp. 504–517.

[10] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Intl. Conf. on Communications, Internet and Information Technology (CIIT)*, St. Thomas, US Virgin Islands, Nov. 22-24 2004, pp. 201–206.

[11] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proc. IEEE Third Intl. Conf. on Security and Privacy in Communications Networks (SecureComm)*, Nice, France, Sep. 17-21 2007, pp. 331–340.

[12] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.

[13] ——, "Bayesian detection of WiFi transmitter RF fingerprints," *Electronics Letters*, vol. 41, no. 6, pp. 373–374, 2005.

[14] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker, "Passive data link layer 802.11 wireless device driver fingerprinting," in *Proc. 15th USENIX Security Symposium*, Vancouver, B.C., Canada, Jul. 31-Aug. 4 2006, pp. 167–178.

[15] J. Hall, "Detection of rogue devices in wireless networks," Ph.D. dissertation, School of Computer Science, Carleton University, Ottawa, Ontario, 2006.

[16] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Intl. Conf. on Mobile Computing and Networking (Mobicom)*, San Francisco, CA, Sep. 14-19 2008.

[17] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 4, pp. 1346–1354, Dec. 2011.

[18] A. Mahmood and M. A. Jensen, "Data-dependent transmitter fingerprints for radio authentication," in *Proc. IEEE Radio and Wireless Symp.*, Newport Beach, CA, Jan. 19-22 2014, pp. 1–3.

[19] *Data Sheet, SMV123x Series: Hyperabrupt Junction Tuning Varactors*. [Online]. Available: http://www.skyworksinc.com/uploads/documents/200058Q.pdf

[20] J.-J. Van de Beek, O. Edfors, M. Sandell, S. K. Wilson, and P. O. Borjesson, "On channel estimation in OFDM systems," in *Vehicular Technology Conference, 1995 IEEE 45th*, vol. 2. IEEE, 1995, pp. 815–819.